

Troy L. Isaacson, Esq., NV Bar No. 6690  
MADDOX ISAACSON & CISNEROS, LLP  
11920 Southern Highlands Parkway, Suite 100  
Las Vegas, Nevada 89141  
Telephone: (702) 366-1900  
Facsimile: (702) 366-1999

Ryan L. Isenberg  
Georgia Bar No. 384899  
Isenberg & Hewitt, P.C.  
6600 Peachtree Dunwoody Road  
600 Embassy Row, Suite 150  
Atlanta, Georgia 30328  
770-351-4400 (Voice)  
770-828-0100 (Fax)  
[ryan@isenberg-hewitt.com](mailto:ryan@isenberg-hewitt.com)

UNITED STATES DISTRICT COURT  
DISTRICT OF NEVADA

ROBERT MILLER,

PLAINTIFF,

V.

4INTERNET, LLC AND  
JOHN DOES 1-10

DEFENDANTS.

AND

4INTERNET, LLC

COUNTERCLAIMANT

V.

ROBERT MILLER, ET. AL.

COUNTERCLAIM DEFENDANTS

CIVIL ACTION FILE

NO. 2:18-cv-02097-JAD-VCF

ORAL ARGUMENT REQUESTED<sup>1</sup>

<sup>1</sup>Counsel for 4Internet will be out of the country from May 16-27.

**RESPONSE TO MOTION TO DISMISS AMENDED COUNTERCLAIMS**

COMES NOW, 4Internet, LLC (“4Internet”) in the above-styled action, and herein files this Response to the Motion to Dismiss 4Internet, LLC’S Amended Counterclaims (Doc. 41), and shows this Court as follows:

**Executive Summary**

In granting the prior motion to dismiss (Doc. 39), the Court found that 4Internet had not pleaded sufficient facts to demonstrate that 4Internet’s alleged harm was caused by the counterclaim defendants, as opposed to a third-party. In the Amended Counterclaim, 4Internet has pleaded specific facts showing that the outages its server suffered were plausibly caused by the Plaintiffs. Specifically, 4Internet has identified specific IP addresses that are associated both with the Higbee law firm and Christopher Sadowski, that there is a correlation between visits from these addresses and an increase in the activity that caused 4Internet’s slowdowns or server outages. The user agent data, when combined with publicly available statements and information, leave little doubt that someone at Higbee & Associates or Christopher Sadowski directed the activity that caused the 4Internet’s problems.

The Counterclaim Defendants raise new arguments in this motion asserting that the claims under the CFAA should be dismissed for failure to state a claim under *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1004 (9th Cir. 2019). *hiQ* discussed the parameters of the definition of without authority under the CFAA. The *hiQ Court* affirmed the grant of a preliminary injunction to a party that was scraping data from LinkedIn, and which discussed the. The Counterclaim Defendants seemingly acknowledge that what 4Internet alleges sounds a lot like a Distributed Denial of Service (“DDOS”) attack. The allegations are that the technology

1 platform aimed and deployed at 4Internet, not to cause harm, but to scrape, caused the same  
2 harm as a DDOS attack, and *hiQ* does not condone the deliberately indifferent deployment of  
3 that technology.

4  
5 Finally, under the Georgia CSPA, the definition of “without authority” is statutorily  
6 defined to be broader than some courts have considered under the CFAA, and those claims  
7 should survive independently.

#### 8 **Statement of Material Facts**

9 4Internet operates a search engine using a recently patented search methodology. This  
10 search engine is comprised of thousands of different domains.<sup>2</sup> During 2018 through September  
11 2019, 4Internet used a single privately hosted<sup>3</sup> computer to manage relatively small amounts of  
12 human internet traffic, which limits the ability of the server to manage unusual spikes in traffic.<sup>4</sup>  
13 Like (presumably) all search engines, 4Internet has a terms of use page that requires visitors to  
14 access the webpages using the system interface, which was visited by someone at Higbee &  
15 Associates.<sup>5</sup> 4Internet captures user data from its visitors. This data includes the date and time  
16  
17  
18  
19  
20  
21

---

22 <sup>2</sup> Doc. 40 ¶ 10-13.

23 <sup>3</sup> As discussed in more detail below, Counterclaim Defendants’ have made several material  
24 misrepresentations to this Court regarding 4Internet’s server. Despite the insistence of the  
25 purportedly qualified computer specialist working for Higbee & Associates, 4Internet’s server is  
26 privately hosted and is not cloud based. Rather, 4Internet uses Cloudflare’s DNS service so that  
when a user on the internet types in a domain like 4baseball.com the user is directed to the  
device associated with the numerical IP address that corresponds to the domain in the DNS  
listing.

27 <sup>4</sup> Doc. 40 ¶ 18-19.

28 <sup>5</sup> Doc. 40 ¶ 68.

1 of the visit, the IP address of the visitor, detailed browser data, display size, and the page on the  
 2 internet the user was immediately preceding the visit to the 4Internet site.<sup>6</sup>

3 Higbee & Associates is a law firm that holds itself out as being a technology driven.<sup>7</sup>  
 4 Copypants is a technology platform that requests pages on the internet and can take screenshots  
 5 of those pages. Copypants, or a similar platform, is a bot that is deployed using Microsoft  
 6 Azure. The user agent for Azure based bots includes, among potentially others, a variation of  
 7 BingPreview.<sup>8</sup> When the Copypants bot visits a page, it uses system resources of the server that  
 8 hosts the page.<sup>9</sup> Copypants can be directed to a particular website.<sup>10</sup> Higbee & Associates  
 9 entered into a relationship with Copypants in 2016 that continued into 2018.<sup>11</sup> In his previously  
 10 filed declaration, Mathew Higbee admitted that he and his firm used Copypants.<sup>12</sup>

13 Visits from Higbee & Associates correspond with visits from Copypants. Prior to April  
 14 30, 2018, 4Internet had little relative bot traffic. On April 30, 2018, 4conservative.com received  
 15 2 visits from IP address 52.184.164.235. The next day, 4search.com received 15 visits from that  
 16 same address with user agent information that included “BotPants” and [info@copypants.com](mailto:info@copypants.com).<sup>13</sup>  
 17 Another visit is recorded on May 2. The visits that are recorded in the spreadsheets in Doc. 35-1  
 18

---

21 <sup>6</sup> Doc. 40 ¶¶ 20, 35, 105; Doc. 35-1 pp. 12-17).

22 <sup>7</sup> Doc. 40 ¶ 25.

23 <sup>8</sup> Doc. 40 ¶¶ 22, 24. The BingPreview Bot data is reflected in the graphs attached to the  
 24 Complaint as Exhibits D-1 through D-5.

24 <sup>9</sup> Doc. 40 ¶ 28.

25 <sup>10</sup> Doc. 40 ¶ 44.

26 <sup>11</sup> Doc. 40 ¶ 29. In an article published in Fast Company, Higbee admits to having used both  
 27 Copypants and his own similar service. See <https://www.fastcompany.com/40494777/here-come-the-copyright-robots-for-hire-with-lawyers-in-tow>

28 <sup>12</sup> Doc. 40 ¶ 66.

<sup>13</sup> Doc. 40 ¶¶ 38-39.

are likely individual users either Higbee employees or clients. On May 3, 2018, the 4Internet server is inundated with BingPreview requests, which slows the server down and causes an outage shortly thereafter.<sup>14</sup>

On July 18, 2018, 4Internet receives 11 separate visits from the same Higbee & Associates IP address. That same day, 4Internet is again inundated with BingPreview visits that causes a slowdown and an outage that largely lasts for a few days.<sup>15</sup> The volume of these visits is so large, measuring in the millions, that it cannot be downloaded into a spreadsheet. 4Internet has tried to graphically display this in Exhibit D-1.<sup>16</sup> Similar activity was seen in August 2018.<sup>17</sup>

4Internet received additional demands on September 10, 2018 for a client named Alex Maxim and another for Christopher Sadowski dated September 24, 2018. Around the time of receiving these new demands, there was a spike in BingPreview bot traffic.<sup>18</sup> On September 25, 2018, Counsel for 4Internet informed Mathew Higbee that whatever technology was seemingly being used was using system resources and had caused a temporary outage.<sup>19</sup>

Higbee is the co-founder of Image Defender, which operates a service that is nearly identical to Copypants.<sup>20</sup> In fact, Image Defender holds itself out as doing a “deep dive” to find potentially infringing material.<sup>21</sup> The bot that 4Internet found and which continued to cause

---

<sup>14</sup> Doc. 40 ¶ 41. The Court should note that these BingPreview and Copyrant Bot visits are measures in the millions and so numerous that they can’t be downloaded into a spreadsheet.

<sup>15</sup> Doc. 40 ¶¶ 43-44.

<sup>16</sup> Doc. 40-1 (P. 6).

<sup>17</sup> Doc. 40 ¶¶ 48-50.

<sup>18</sup> Doc. 40 ¶¶ 54-55; Doc. 40-1 (Ex. D-3).

<sup>19</sup> Doc. 40 ¶ 71.

<sup>20</sup> Doc. 40 ¶¶ 21-33.

<sup>21</sup> Doc. 40 ¶ 57.

1 harm after August 2018 had, in its user agent, Azure IP addresses, a variation of BingPreview,  
2 and highly unusual screen display ratios.<sup>22</sup>

3 On March 13, 2019, 4Internet received another legal demand from Higbee & Associates  
4 relating to Christopher Sadowski.<sup>23</sup> This demand, like the ones the previous September,  
5 corresponds to a significant increase in bot activity and caused an actual outage.<sup>24</sup> The bot  
6 activity decreased substantially in September 2019, but not before 4Internet had spent over a  
7 thousand hours trying to defend itself from the bot activity.<sup>25</sup>

### 8 **Argument and Citation to Authority**

#### 9 **I. 4Internet States a Claim for Relief under Article III**

10 The Court, in its Order (Doc. 39 at 12-14), expressed concern, relying *Maya v. Centex Corp.*,  
11 658 F.3d 1060, 1072 (9th Cir. 2011) that 4Internet had not pleaded sufficient facts for the Court  
12 to find that the harm alleged by 4Internet was plausibly caused by the Counterclaim Defendants.  
13 Under *Maya*, “to survive a motion to dismiss for lack of constitutional standing, plaintiffs must  
14 establish a “line of causation” between defendants’ action and their alleged harm that is more  
15 than “attenuated . . .” *Id.* at 1070. There is nothing to suggest there are any attenuated facts in  
16 the case before the Court. There is no allegation or any showing of any third-party conduct that  
17 would have intervened to cause 4Internet’s harm, and all that’s necessary is that 4Internet allege  
18 facts that “support an actionable causal relationship between [the Counterclaim Defendants’]  
19 conduct and [4Internet’s] asserted injury.” *Warth v. Seldin*, 422 U.S. 490, 507 (1975).  
20  
21  
22  
23  
24

---

25 <sup>22</sup> Doc. 40 ¶¶ 60, 69.

26 <sup>23</sup> Doc. 40 ¶ 56.

27 <sup>24</sup> Doc. 40-1 (Ex. D-5).

28 <sup>25</sup> Doc. 40 ¶¶ 59, 75.

1 In its Amended Counterclaim, 4Internet has alleged and identified numerous facts that  
 2 address the Court's concerns. Underlying these facts is data captured by 4Internet from its  
 3 visitor logs. This data includes the IP address of the visiting device, detailed browser data,  
 4 display size, and the page on the internet the user was immediately preceding the visit to the  
 5 4Internet site, which is referred to as a referrer string.

7 There are two sets of data. One set is from users who appear to have manually visited the  
 8 relevant site. For instance, in Exhibit B (Doc. 40-1), a user associated with Higbee & Associates  
 9 visited a page within the 4search.com domain. The page visited is actually located on the  
 10 chicago.cbslocal.com server. The first row shown in Exhibit B is known to be associated with  
 11 Higbee & Associates because the referrer string shows that the page immediately before the  
 12 4search page was copyright.higbeeassociates.com/case\_screening . . . , which will take you to a  
 13 login page at the Higbee website.<sup>26</sup> The second row in Exhibit B shows a visit to the exact same  
 14 page from an IP address<sup>27</sup> that in prior earlier visits included in the user agent the following:  
 15 [compatible; BotPants/1.0; Linux; +info@copypants.com<sup>28</sup>].

17 The second set of data received is enormous and can't be downloaded into a spreadsheet  
 18 given its sheer volume. 4Internet has attempted to graphically demonstrate these visits and their  
 19 impact in Exhibits D-1 through D-5. Essentially, 4Internet has, from the data it happens to have  
 20 captured, keeping in mind that these are unintentional bread crumbs that happen to have been left  
 21

---

24 <sup>26</sup> Though 4Internet can't authenticate this itself, the IP, when subjected to a geolocation search  
 25 shows it belongs to Charter Communications, and is assigned to the Law Firm of Higbee &  
 Associates in Santa Ana, California.

26 <sup>27</sup> This IP address resolves back to Microsoft, which indicates its associated with someone using  
 Microsoft Azure.

27 <sup>28</sup> See, e.g. Doc. 35-1 (p.6 Line 19)

1 behind, alleged that visitors from Higbee & Associates, or someone with access to the Higbee &  
2 Associates platform, starts out theoretically looking for potential infringing material<sup>29</sup> and then  
3 directs the technology platform, whether it was Copypants, Image Defender, or some other  
4 similar program, to do its “deep dive.”<sup>30</sup> Whatever this activity is thought to be, which Mr.  
5 Higbee acknowledged not understanding, the practical impact is that it bombarded 4Internet’s  
6 server with page requests to the point that the server was crippled or taken offline altogether.<sup>31</sup>  
7 The use of Azure, the user agent data, the use of Apple computer products, the use of technology  
8 by Higbee & Associates, and the fact that Higbee & Associates and Christopher Sadowski do  
9 this for a living are sufficient facts for the Court to find that it is plausible that Higbee &  
10 Associates used technology that caused 4Internet’s slowdowns and outages.<sup>32</sup> In virtually all of  
11 the cases where the element of causation is discussed in connection with Article III standing  
12 there is some broad policy-based concern before the Court. In *Maya*, the issue was whether  
13 homeowner could sue developers for marketing homes to buyers who were likely to be  
14 foreclosed upon thus causing a decrease in the value of the Plaintiffs’ homes. The question is  
15  
16  
17  
18  
19

---

20 <sup>29</sup> Given the trollish behavior of these Counterclaim Defendants, it is more likely they are just  
21 looking for any display of seeded photographs without regard to copyrightability or  
22 infringement.

23 <sup>30</sup> See Exhibit C-1.

24 <sup>31</sup> This is what their own “expert” acknowledges looked like a DDOS attack. 4Internet is not  
25 alleging that the Counterclaim Defendants intended such an attack, only that this was the result  
26 of their scraping technology, they were told it was causing harm, but continued.

27 <sup>32</sup> Take a run of the mill slip and fall case at Walmart in which the Plaintiff alleges a slip and fall  
28 and an injury that requires surgery. It may well be that the surgical intervention was not caused  
by the fall, but was caused by the aging process. See, e.g. *Stedeford v. Wal-mart Stores, Inc.*,  
No. 214CV01429JADPAL, 2016 WL 3844211, at \*1 (D. Nev. July 15, 2016). Article III  
standing does not require such a Plaintiff to affirmatively eliminate other potential causes in a  
pleading.

1 whether the Court can find that the harm caused to 4Internet's was the "result of the independent  
2 action of some third party not before the court." See *Pritikin v. Dep't of Energy*, 254 F.3d 791,  
3 797 (9th Cir. 2001) citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992). 4Internet has  
4 averred specific facts that allow it to allege that it was harmed by technology that, based on all  
5 available evidence, points to Higbee & Associates. If Higbee & Associates used a third-party to  
6 direct its scraping activities at 4Internet, that would only mean that 4Internet would have another  
7 party to sue. It would not remove Higbee & Associates from the chain of causation.

9 II. 4Internet States a Claim under the CFAA

10 The Counterclaim Defendants move to dismiss 4Internet's claims under the Computer Fraud  
11 and Abuse Act ("CFAA") and the Georgia Computer Systems Protection Act ("CSPA") under  
12 F.R.C.P. § 12(b)(6). The argument is seemingly based entirely on the recent decision of the  
13 Ninth Circuit in *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1001 (9th Cir. 2019). In  
14 *LinkedIn*, hiQ scraped data about LinkedIn's users from publicly accessible pages. LinkedIn  
15 sent a cease and desist letter to hiQ and asserted any further scraping was without authorization  
16 and a violation under CFAA. hiQ filed for a declaratory judgment and was granted a preliminary  
17 injunction that precluded LinkedIn from denying hiQ access to publicly available LinkedIn  
18 member profiles. LinkedIn raised as a defense that the CFAA preempted the state law tort  
19 claims that had been asserted. In analyzing this issue, the *LinkedIn Court* considered the  
20 meaning of the CFAA's reference to "without authorization." In what can only be described as  
21  
22  
23  
24  
25  
26  
27  
28

dicta,<sup>33</sup> the Court, relying on a 1984 congressional report, found that what was required was something closer to breaking and entering.<sup>34</sup>

The relevant phrase in the CFAA prohibits individuals from accessing a “computer without authorization or exceeding authorized access . . .” 18 U.S.C. § 1030. These phrases are not ambiguous, which should preclude any further inquiry. *Rotkiske v. Klemm*, 140 S. Ct. 355, 360 (2019) (citation omitted). Regardless, the Court is required to give effect to the clear meaning of the statute, and “begin and end [its] inquiry with the text, giving each word its ordinary, contemporary, common meaning.” *Star Athletica, L.L.C. v. Varsity Brands, Inc.*, 137 S. Ct. 1002, 1010 (2017) (citations and quotation marks omitted). No mental gymnastics are required to determine what the relevant phrase means, nor how it should be interpreted, or applied. Without means “to not have,”<sup>35</sup> and authorization means permission.<sup>36</sup> One either has permission (authorization) or not, and if one does not have permission then that party is without authorization.

“When a statute includes an explicit definition, [the Court] must follow that definition,” even if it varies from a term's ordinary meaning.” *Digital Realty Tr., Inc. v. Somers*, 138 S. Ct. 767,

---

<sup>33</sup> *LinkedIn* at 1000 (At the very least, we conclude, hiQ has raised a serious question as to this issue.)

<sup>34</sup> In *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 585 (1st Cir. 2001) in a case discussing whether a scraper caused damage, the First Circuit noted that an interpretation suggested by the appellant “would flout Congress's intent by effectively permitting the CFAA to languish in the twentieth century, as violators of the Act move into the twenty-first century and beyond.” Considering the average age of the congressional representatives who signed on to a report in 1984 about what computer hacking looked like then and applying it now instead of the text is, at the very least, troubling.

<sup>35</sup> <https://dictionary.cambridge.org/us/dictionary/english/without>

<sup>36</sup> <https://dictionary.cambridge.org/us/dictionary/english/authorization>

1 776 (2018). To exceed authorization under 18 U.S.C. § 1030(e)(6) means “to access a computer  
2 with authorization and to use such access to obtain or alter information in the computer that the  
3 accesser is not entitled so to obtain or alter.”

4  
5 4Internet’s terms of use page required visitors to only access it’s the pages in its site using  
6 the system interface, and the visitors from the Higbee & Associates IP addresses visited these  
7 pages on multiple occasions.<sup>37</sup> On September 25, 2018, Higbee & Associates was informed that  
8 the technology was causing problems and that such use exceeded the authorization granted under  
9 18 U.S.C. § 1030(a)(5).<sup>38</sup> Despite having been specifically informed of this, Higbee &  
10 Associates continued to deploy the technology in February and March and seemingly into  
11 September of 2019.<sup>39</sup>

12  
13 In *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067-68 (9th Cir. 2016), the  
14 Ninth Circuit seems to have synthesized holdings in *LVRC Holdings LLC v. Brekka*, 581 F.3d  
15 1127 (9th Cir. 2009) and *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012). It discerned two  
16 rules. First, “a defendant can run afoul of the CFAA when he or she has no permission to access  
17 a computer or when such permission has been revoked explicitly. Once permission has been  
18 revoked, technological gamesmanship or the enlisting of a third party to aid in access will not  
19 excuse liability. Second, a violation of the terms of use of a website—without more—cannot  
20 establish liability under the CFAA.”  
21  
22  
23  
24  
25

26 <sup>37</sup> Doc. 40 ¶ 68.

27 <sup>38</sup> Doc. 40 ¶ 71.

28 <sup>39</sup> Doc. 40-1 (D-4, D-5); Doc. 40 ¶ 59.

1 The *Facebook Court* then went on to affirm that liability was possible after Facebook had  
2 sent Power Ventures a cease and desist letter, and Power Ventures continued to access  
3 Facebook's computers knowing that it was not authorized to do so. Though it is clear that Ninth  
4 Circuit precedent precludes liability under the CFAA for merely violating the terms of use of a  
5 website, *Facebook* informs us that telling the violating party to stop is sufficient.  
6

7 In his declaration filed previously with the Court (Doc. 25-2), Mr. Higbee admitted he really  
8 didn't know how Copypants worked.<sup>40</sup> No effort has been made to explain what the technology  
9 is that they use (which as a matter of common sense seemingly would be Image Defender), how  
10 its deployed, or how they understand it works. Instead, aside from their general denials, they  
11 question Internet's factual assertions and victim blame it for not having better defenses. Even  
12 before Internet informed him that the technology that was being used was causing problems,  
13 that he chose not to understand how it worked is deliberate indifference, which satisfies any  
14 knowledge requirement under the CFAA. See *United States v. Nosal*, 844 F.3d 1024, 1039 (9th  
15 Cir. 2016) (*We have repeatedly held that a statutory requirement that a criminal defendant acted*  
16 *"knowingly" is "not limited to positive knowledge, but includes the state of mind of one who*  
17 *does not possess positive knowledge only because he consciously avoided it)* (citations omitted).  
18 Certainly, once he was so informed, Mr. Higbee and his firm had an affirmative duty to  
19 investigate whether it was causing harm, and the failure to do so would satisfy the knowledge  
20 requirement under the CFAA, which can be generally averred under Rule § 8(a).  
21  
22  
23  
24

---

25 <sup>40</sup> This same declaration is word-smithed to give the Court the impression that Copypants wasn't  
26 operating after September 2018, but what he actually says is that "its freelance services" and  
27 "website" were down. He does not deny using the Copypants technology, or developing his  
28 own.

1 In *Starr v. Baca*, 652 F.3d 1202 (9th Cir.2011) the Ninth Circuit (discussing the sufficiency  
2 of a pleading under *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007) held that where there  
3 are two alternative explanations, one by each party, then the complaint survives. 4Internet has  
4 asserted specific facts that demonstrate that someone having access to the Higbee & Associates  
5 technology platform deployed its bot after being told that it was causing harm, and this continued  
6 after being told that such use exceeded any authorization that had been granted. 4Internet has  
7 specifically alleged that Higbee & Associates' technology was scraping large amounts of data,  
8 which after being told that this exceeded authorization, fits within the definition provided in 18  
9 U.S.C. § 1030(e)(6).  
10

11 4Internet has alleged that Higbee & Associates uses a technology platform to search for  
12 targets, and that this platform is controlled through Microsoft Azure. Azure uses BingPreview.  
13 The bot that caused 4Internet's problems contain a variation of BingPreview in the user agent.  
14 4Internet has alleged that it had little bot traffic to speak of prior to April 30, 2018, and further  
15 alleged that spikes in bot traffic around times it receives demand letters from Higbee &  
16 Associates. This is not a coincidence and 4Internet has plausibly demonstrated that someone  
17 with access to the Higbee & Associates system, after Higbee & Associates was told that it had  
18 exceeded authorization by using their technology, continued to deploy the technology without or  
19 exceeding authorization, which caused harm.  
20  
21

22 4Internet's has averred specific facts that would satisfy the damage threshold requirements as  
23 well.<sup>41</sup> See *Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010)  
24  
25

---

26  
27 <sup>41</sup> Doc. 40 ¶¶ 75-79.  
28

(citations omitted) (*It is sufficient to show that there has been an impairment to the integrity of data, as when an intruder retrieves password information from a computer and the rightful computer owner must take corrective measures “to prevent the infiltration and gathering of confidential information.”*).

Finally, the Counterclaim Defendants take the position that what 4Internet appears to be complaining about is a denial of service attack. Such an attack would give rise to liability under the CFAA. See *BHRAC, LLC v. Regency Car Rentals, LLC*, No. CV 15-865-GHK MANX, 2015 WL 3561671 (C.D. Cal. June 4, 2015); *Tyco Int'l (US) Inc. v. John Does, 1-3*, No. 01 CIV.3856(RCC)(DF), 2003 WL 23374767, at \*1 (S.D.N.Y. Aug. 29, 2003). Given the facts 4Internet has alleged, it would have been entitled to expedited discovery had it merely filed a John Doe action. See *Ebates, Inc. v. Does*, No. 16-CV-01925-JST, 2016 WL 2344199 (N.D. Cal. May 3, 2016). This is true outside the denial of service arena under the CFAA. See, e.g. *Uber Techs., Inc. v. Doe*, No. C 15-00908 LB, 2015 WL 1205167, at \*2 (N.D. Cal. Mar. 16, 2015).

### III. The Declaration of Jason Dora (1) is Wrong and (2) Cannot be Considered.

As the Court is well aware, in considering a Motion to Dismiss under Rule § 12(b)(6), review is limited to the complaint's factual allegations. Factual challenges have no bearing on the analysis. *Lee v. City of Los Angeles*, 250 F.3d 668, 688 (9th Cir. 2001). Despite this standard, the Counterclaim Defendants have submitted, and rely upon, the declaration of a recently hired employee who is holding himself out as a technology expert, and who presents his own explanation for why 4Internet's facts are wrong. Notwithstanding that the contents of the declaration cannot be considered; the declarant has gotten many of his facts wrong. Essentially, Mr. Dora explains that 4Internet uses Cloudflare and Cloudflare protects its users against a

1 DDOS Attack,<sup>42</sup> which presumably he believes is what 4Internet suffered. But, 4Internet only  
2 uses Cloudflare for its Domain Name Server and reverse proxy service (1) so that users can find  
3 the 4Internet pages without revealing what the actual IP address is for the server and (2) for  
4 security purposes. To be clear, as has been alleged, 4Internet's server is not cloud-based.

5  
6 In addition, Mr. Dora's assumption about Cloudflare's DDOS defenses are also misplaced.  
7 First, the mitigation doesn't help at all if the attacking party knows the IP address of the target,  
8 and second, the defenses mitigate against very large attacks.<sup>43</sup> Though the deployment of the  
9 technology here caused problems for a single server system, this was by no means a "very large  
10 attack." It is possible that an enterprise version of Cloudflare may provide some additional  
11 protection, but 4Internet does not, and does not have the resources to, subscribe to that tier of  
12 service.  
13

14 One other issue that Mr. Dora doesn't know, understand, or appreciate, is that the vast  
15 majority of 4Internet's pages are dynamically created in real time. Apparently, neither the  
16 photoshop, nor software engineering certificate programs that Mr. Dora attended, included  
17 curriculum on how to account for the time and resources associated with dynamically created  
18 pages.  
19  
20  
21  
22

---

23  
24 <sup>42</sup> 4Internet does not allege that the Higbee Defendants engaged in a DDOS attack. Rather,  
25 4Internet alleges that Defendants, even if they didn't understand at the beginning, were told, that  
26 the technology platform they were using to presumably look for infringing materials on the  
27 4Internet sites was using substantial system resources and causing harm.

28 <sup>43</sup> [https://support.cloudflare.com/hc/en-us/articles/200170196#h\\_dfff923a-5879-4750-a747-ed7b639b6e19](https://support.cloudflare.com/hc/en-us/articles/200170196#h_dfff923a-5879-4750-a747-ed7b639b6e19)

1 And, not to address all of the issues he has raised, but the impact of Google’s web crawler  
2 (which does not visit as often as Dora would seemingly believe) visiting compared with the  
3 impact of this particular bot visiting are also not the same.

4  
5 IV. Georgia CSPA

6 Under the Georgia CSPA, regardless of how the Court interprets or applies the without or  
7 exceeds authorization under the CFAA, 4Internet has stated a claim because the definition of  
8 without authority is indisputably broader in scope. OCGA § 16-9-93(b) provides that

9 [a]ny person who uses a computer or computer network with knowledge that such  
10 use is without authority and with the intention of: (1) Deleting or in any way  
11 removing, either temporarily or permanently, any computer program or data from  
12 a computer or computer network; (2) Obstructing, interrupting, or in any way  
13 interfering with the use of a computer program or data; or (3) Altering, damaging,  
14 or in any way causing the malfunction of a computer, computer network, or  
15 computer program, regardless of how long the alteration, damage, or malfunction  
16 persists[,] shall be guilty of the crime of computer trespass.

17 Subsection (g)(1) allows “[a]ny person whose property or person is injured by  
18 reason of a violation of any provision of this article [to] sue therefor and recover  
19 for any damages sustained and the costs of suit.

20 OCGA § 16-9-92(18) defines “[w]ithout authority” to include “the use of a computer or  
21 computer network in a manner that exceeds any right or permission granted by the owner of the  
22 computer or computer network.” *Gryder v. Conley*, 836 S.E.2d 120, 127 (Ga. Ct. App. 2019)  
23 (emphasis added). Georgia law requires the Court to apply the plain and ordinary meaning of  
24 words to statutory text. See *Tibbles v. Teachers Ret. Sys. of Georgia*, 297 Ga. 557, 558 (2015).  
25 Under this doctrine or that set forth in *Digital Realty Tr., Inc. v. Somers*, *infra*, the Georgia  
26 definition of “without authority” permits 4Internet to bring its claim against those parties who  
27 knowingly exceeded the permission granted and caused any malfunction or damage. 4Internet  
28 has alleged that the Counterclaim Defendants exceeded the authority granted and caused harm.

V. 4Internet Should Be Permitted to Amend to Add Claims, If Not Under The CFAA

The *HiQ Court*, *infra* at 1005, noted that “entities that view themselves as victims of data scraping are not without resort, even if the CFAA does not apply: state law trespass to chattels claims may still be available. And other causes of action, such as copyright infringement, misappropriation, unjust enrichment, conversion, breach of contract, or breach of privacy, may also lie.” Of course, some of these would not apply, but intentionally continuing to deploy a harmful technology after being told its causing harm should be actionable under state law.

In addition, should the Court seek additional facts, 4Internet can analyze the millions of bot visits for more detail<sup>44</sup> (but would need substantially more than a couple of weeks to re-plead) and can plead that based on this analysis and the lack of previous bot traffic that it is unlikely that there was any other source for the bot visits that caused its slowdowns and outages, though these inferences can be fairly taken from the operative counterclaim.

VI. Claims Against Christopher Sadowski

4Internet has pleaded facts that show that it was the subject of unauthorized and harmful bot traffic that likely originated from Higbee & Associates. Christopher Sadowski has been identified as having an interest in this case and is a professional litigant. 4Internet has identified an IP address is likely to have been used by Christopher Sadowski that shows that he had access to the Higbee & Associates technology platform.<sup>45</sup> The “plausibility standard [ . . . ] does not prevent a plaintiff from pleading facts alleged upon information and belief where the facts are

---

<sup>44</sup> If this were a John Doe case and 4Internet obtained discovery, it would be much easier to match up the information it has captured with the information obtained from Microsoft or the Defendants.

<sup>45</sup> Doc. 40 ¶¶ 93, 102-107.

Should the Court find that Christopher Sadowski cannot be liable to 4Internet, 4Internet concedes that its claim for declaratory judgment should be transferred to the District of New Jersey<sup>46</sup> or can be dismissed without prejudice. See *Reed v. Brown*, 623 F. Supp. 342, 345–46 (D. Nev. 1985); *Goldlawr, Inc. v. Heiman*, 369 U.S. 463, 466 (1962) (Court can transfer a case under 28. U.S.C. § 1404 or § 1406 even where it lacks personal or subject matter jurisdiction).

15 Conclusion

What happens if the Court grants the motion and it turns out 4Internet was right that the someone at Higbee & Associates or one of that firm's regular clients who has access to the technology platform did in fact turn on the spicket that flooded 4Internet with bot traffic that shut down its website? The answer is most assuredly not justice. Parties are not required to prove their case in their pleading and in fact are permitted to be wrong, and are permitted to lose. A party could bring a claim and remember the facts wrong, but they aren't precluded from having their day in court.

<sup>46</sup> See Sadowski v. Alpha Media, LLC (Dist. of Oregon), Case No. 3:2019CV01646 ([Doc. 1](#)).

1 4Internet installed proprietary systems on its servers that coordinate closely with other  
2 web information providers and record data at both the server and client level. This allows for  
3 advanced tracking of web visits and the back-tracing of user originations. Because 4Internet is in  
4 control of every part of its custom-built servers, kernels, and applications it has tracking  
5 capabilities far beyond what would be considered standard. These systems provide detailed  
6 information not typically tracked by web servers and administrators. This data, found in multiple  
7 database tables with millions of rows, is too large to provide to the court. As 4Internet has  
8 revealed some of its capabilities in filings in this case, it has become apparent that Higbee is  
9 adapting its methods by blocking user agent information and referrer string data. Regardless,  
10 with the information available to it, 4Internet has put enough of the puzzle pieces together to  
11 show it is plausible that the harm it suffered from bot traffic at levels not seen before the Higbee  
12 visits started, originated from Higbee & Associates.

15 In its prior order, the Court noted that the facts as previously pleaded “show at best that it  
16 is merely possible that Higbee and H&A's use of Copyants, as opposed to a third party's use, is  
17 what took down 4Internet's server.” 4Internet is not required to plead with certainty that the  
18 Counterclaim Defendants caused the harm it suffered. It is only required to plead facts that make  
19 it plausible—not even probable. Hackers can use virtual private networks and other tools to  
20 mask their location and identity. 4Internet did not randomly pick the Counterclaim Defendants  
21 out of a hat. They admit to using technology in connection with what they will argue are  
22 legitimate efforts to find infringements. These Defendants file an awful lot of lawsuits and it is  
23 certainly not outside the realm of the plausible that the technology they use could cause harm to  
24 4Internet's web server as alleged. 4Internet analyzed the data it had which circumstantially show  
25 it was in fact these Defendants that caused its harm. 4Internet alleged that it had no bot traffic to  
26  
27  
28

1 speak of until after it was visited by these Defendants. Is it possible that it was some unknown,  
2 unnamed third-party that had nothing to do with these Defendants? Sure. But, it's also possible  
3 that when a plaintiff alleges that a defendant ran a red light that the defendant had a green light  
4 or that the lights at the intersection were faulty. The Counterclaim Defendants Motion to  
5 Dismiss should be denied.  
6

7 WHEREFORE, 4Internet prays that the Court deny the Motion to Dismiss, allow further  
8 amendments if appropriate, and for such other and further relief as justice requires.

9 Dated this the 21<sup>st</sup> day of February, 2020.

10 /s/ Ryan Isenberg  
11 Ryan L. Isenberg

12 **Certificate of Service**

13 This is to certify that I have this day served the within and foregoing Response to the  
14 Motion to Dismiss 4Internet, LLC's Amended Counterclaims upon Plaintiff and Counterclaim  
15 Defendants by filing the same using the CM\ECF system, which will generate notice to the  
16 following counsel of record:  
17

18 Mathew K. Higbee, Esq.  
19 HIGBEE & ASSOCIATES  
20 3481 E Sunset Rd., Suite 100  
Las Vegas, NV 89120

21 /s/ Ryan Isenberg  
22  
23  
24  
25  
26  
27  
28